



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/063,891 | 05/22/2002 | Kun-Huei Chen | IACP0004USA | 2371 |

27765 7590 12/14/2005

NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION
P.O. BOX 506
MERRIFIELD, VA 22116

| |
|----------|
| EXAMINER |
|----------|

DAVIS, ZACHARY A

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2137

DATE MAILED: 12/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|--|-------------------------------|-----------------------------|--|
| <p align="center">Office Action Summary</p> | Application No. 10/063,891 | Applicant(s) CHEN ET AL. | |
| | Examiner Zachary A. Davis | Art Unit 2137 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 May 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>20050223</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: Throughout the specification, for example, in the abstract; on page 4, paragraph 0011; and in Claim 1, the term "detonate" is used. The Examiner notes that "detonate" is defined as "explode" or "cause to explode". It appears that this is not the intended meaning of the term; it is assumed that it is intended to mean "start" or "activate".

Appropriate correction is required. Applicant's cooperation is asked in correcting any other errors of which Applicant may become aware in the specification.

Claim Objections

2. Claim 1 is objected to because of the following informalities: the Claim uses the term "detonating". It appears that this is intended to read, for example, "starting" or "activating". Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "an access point connected to the server for transmitting data received from the server via wireless transmission". It is unclear whether the data is received from the server via wireless transmission or whether the data is transmitted from the access point via wireless transmission (or both). This renders the claim indefinite.

Claim 6 recites the limitation "the corresponding identification data". There is insufficient antecedent basis for this limitation in the claims.

All other claims are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Duda, US Patent 5708710 in view of Kung et al, US Patent 6889321.

In reference to Claim 1, Duda discloses a method for updating a ciphering key used in a wireless network system (see, for example, column 3, lines 31-38) where the

method includes starting a counter (column 4, lines 43-48), randomly generating a second key (see column 4, lines 10-12) if the counter conforms to a predetermined threshold (column 4, lines 53-55), a wireless access point transmitting the second key to a wireless station to update a first key stored in the station, and using the updated key to encrypt data between the access point and the station (column 5, lines 34-39). However, although Duda discloses a counter and a counter threshold as described above, Duda does not explicitly disclose that the counter counts a time and that the key is updated at a predetermined time.

Kung discloses a system in which a randomly generated encryption key (column 33, lines 8-11) in a wireless system (see, for example, column 5, lines 14-19) is updated at predetermined time intervals, either a set interval or random sized intervals (column 34, lines 25-43). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Duda to include a clock counting a specific time as the counter, in order to prevent a compromised key from causing excessive damage by limiting the length of time an exposed key would remain active (see Kung, column 34, lines 43-46, where a hacker with access to a broken key is prevented from having continuous access to the system).

In reference to Claims 2 and 3, Duda further discloses transmitting a challenge text from the access point to the station; the station encrypting the challenge text into the response text which is transmitted to the access point; the access point comparing the response text to a standard text, which is also the encrypted challenge text (see column 2, lines 22-32, where a well-known challenge response method is used); the

station transmitting identification data to the access point and thereby to a server; and the access point updating the key if the identification data matches data stored in the server (see column 1, lines 39-50; column 3, lines 45-52; column 4, lines 18-27).

In reference to Claim 4, Duda further discloses requesting a response from a user before updating the key (see column 2, lines 22-32).

In reference to Claim 5, Duda further discloses decrypting data using the second key once the key is updated (column 5, lines 34-39, where the key is updated).

In reference to Claim 6, Duda further discloses a plurality of stations, each storing a key and a unique identification data (column 1, lines 39-48; column 3, lines 45-67).

In reference to Claim 7, Duda further discloses generating the key randomly (column 4, lines 10-12), and Kung also discloses generating the key randomly (column 33, lines 8-11).

In reference to Claim 8, Duda further discloses the access point transmitting a challenge text to the station after the key is updated, and performing a well-known challenge response protocol to verify the second key has been properly received and updated (see column 2, lines 22-32).

In reference to Claim 9, Kung further discloses a real time clock (column 9, lines 55-62).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Raith, US Patent 5241598, discloses a system for synchronizing updated rolling keys in a cellular network.
- b. Rosauer et al, US Patent 5768380, discloses a method for sending updated parameters, including encryption keys, to stations in a wireless network.
- c. Menezes et al, *Handbook of Applied Cryptography*, discloses well-known challenge-response protocols.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER